المحاضرة السادسة: أمن وحماية أنظمة المعلومات

1. ماهية أمن أنظمة المعلومات
2. وسائل حماية أنظمة المعلومات

ماهية أمن أنظمة المعلومات

أ. تعريف أمن نظام المعلومات:

يعد موضوع أمن نظم المعلومات من المواضيع ذات الأهمية البالغة في الوقت الحالي، ذلك أنه يمس بشكل مباشر حياة كل المتعاملين مع الوسائط الإلكترونية بما فيهم مؤسسات الأعمال، وينعكس على مصالحهم وسبل أدائهم لأعمالهم. ولقد وردت العديد من التعاريف التي تخص أمن أنظمة المعلومات نذكر منها:

- ✓ أمن نظام المعلومات هو مجموعة من المناهج، التقنيات والأدوات التي تسمح بحماية موارد النظام المعلومات من أجل ضمان توافر المعلومات سريتها وسلامة محتواها.
- ✓ كما عرف أمن المعلومات حسب وكالة الأمن القومي الأمريكي بأنه حماية أنظمة المعلومات ضد أي وصول غير مرخص إلى المعلومات أو أي تعديل غير مرخص لهذه المعلومات أثناء حفظها ومعالجتها ونقلها، وضد منع تقديم الخدمة لصالح المستخدمين المخولين أو تقديم الخدمة لأشخاص غير مخولين بما في ذلك جميع الإجراءات الضرورية لكشف ومواجهة المخاطر والاعتداءات.
- ✓ أمن نظام المعلومات يعني كل السياسات والإجراءات والأدوات التقنية التي تستخدم لحماية النظام من كل أشكال الاستخدام غير الشرعي للموارد مثل السرقة، التغيير والتعديل، إلحاق الضرر بالمعلومات أو قواعد البيانات أو إلحاق الضرر المادي المتعمد بالأجهزة بالإضافة إلى وجود تهديدات أخرى مثل الأخطاء الإنسانية والحوادث الطبيعية والكوارث.
- ✓ من زاوية أكاديمية يعرف أمن نظام المعلومات بأنه العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها، ومن زاوية تقنية هو عبارة عن الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية.
- ✓ أمن نظام المعلومات هو عبارة عن العمليات والتدابير والتوجيهات التي تصدرها إدارة المؤسسة بهدف حماية مواردها التقنية وما تحتويه من معلومات في مختلف أشكالها بغرض تحقيق سلامتها وتوافرها وسريتها.

ومن خلال التعاريف السابقة يمكن القول أن أمن نظام المعلومات هو مجموعة التدابير والإجراءات التي تتخذها المؤسسة بهدف حماية مواردها التقنية وما تحتويه من معلومات من كل استخدام غير

مرخص كالتخريب والتغيير والسرقة والتلف والضياع والاستخدام غير المرخص وغير القانوني وذلك بالاعتماد على وسائل تقنية وأدوات تضمن لها الوصول إلى الحماية.

وبذلك فأمن نظام المعلومات يهدف إلى:

- ✓ منع انتشار المعلومات بطريقة غير شرعية؛
- ✓ منع تغيير المعلومات وتعديلها بطريقة غير مرخصة؛
- ✓ منع الاستعمال غير المرخص للموارد المعلوماتية والشبكات.

ب. أسباب الحاجة إلى أمن نظام المعلومات:

إن أمن المعلومات ضرورة ملحة ظهرت الحاجة إليها من خلال الأسباب الآتية:

- ✓ **حماية الأصول المعلوماتية الحرجة**، حيث تتضمن المنشأة على أصول معلوماتية مهمة وحرجة يجب حمايتها من أي أخطار تهددها ويجب المحافظة على استمراريتها وبقائها متاحة ومتوافرة في جميع الأوقات، فالحاجة لحماية هذه الأصول تأتي من وجهين، الوجه الأول أنه لا يمكن للمنشأة أن تستمر دون بقاء هذه الأصول عاملة متاحة آمنة والوجه الآخر أن توفير هذه الأصول كلف مبالغ وجهود كبيرة تستحق أن يبذل من أجلها الوقت والجهد والمال لحمايتها، ومن الأمثلة على هذه الأصول المعلومات الحرجة ما يلي: مراكز البيانات، قواعد البيانات، أجهزة الخوادم الرئيسية، شبكات المعلومات المحلية والواسعة، أنظمة التشغيل، البرامج التطبيقية، أجهزة تخزين المعلومات، المواقع والبوابات الإلكترونية سواء داخلية أو على شبكة الإنترنت.

- ✓ **حاجة أعمال المنشآت وأنشطتها إلى ذلك**، حيث أصبحت المعلومات تشكل ثروة حقيقية للمنشآت وموردا مهما من مواردها بل إن المعلومات في بعض المنشآت هي مصدر الدخل الأول لها ويقوم عليها نشاط المنشأة الأساسي والتجارة الالكترونية خير مثال على ذلك؛

- ✓ **حاجة المستفيدين من الخدمات الإلكترونية** لحماية معلوماتهم من كل ما يضر بها، فعندما ينهي شخص معاملاته البنكية أو يشتري سلعة من منزله فإنه لابد أن يعتمد على أمن المعلومات في المحافظة على خصوصيته كاسم المستخدم، كلمة المرور، معلومات البطاقة الائتمانية؛

- ✓ **انتشار الخدمات الالكترونية عن بعد**: مثل خدمات الحكومات الالكترونية والتعليم عن بعد، لدرجة أن المواطن يستطيع أن ينهي جل أو جميع إجراءاته وأن يحصل على درجته العلمية المناسبة من منزله ولإتمام هذا النوع من الخدمات فلابد من توفير الحماية اللازمة للمعلومات ولجميع الأنظمة والتجهيزات التي تخزنها أو تعالجها أو تنقلها لدى كل مقدم الخدمة والمستفيد على حد سواء؛

- ✓ **الحاجة إلى معرفة إمكانيات المؤسسات** ومدى قدرتها على حماية معلوماتها ومعرفة التهديدات التي تواجهها، فلكي تكون آمنا لابد أن تعف نفسك وتعرف التهديدات التي تواجهك ومن هنا جاءت الحاجة إلى أمن أنظمة المعلومات الذي من خلاله يمكن تقويم وضع الحماية في المنشأة ومعرفة التهديدات التي تواجهها وتحليل المخاطر المحيطة بها من أجل أخذ التدابير اللازمة لمجابهة تلك التهديدات والمخاطر؛
- ✓ **كثرة التهديدات المعلوماتية** وتنوعها وتعدد مصادرها، حيث قد توجد جملة من التهديدات داخل المنشأة في أنظمتها المعلوماتية إذا لم يحتاط لها فقد تضر بالمعلومات؛
- ✓ **انتشار الهجمات الالكترونية**، وهي برامج خبيثة تستقر على نظام معلومات المؤسسة من أجل إصابته وإلحاق الضرر بسرية أو سلامة أو توافر معلومات هذا النظام؛
- ✓ كثير من نظم المعلومات لم تصمم بطريقة آمنة لهذا يجب أن يدعم النظام بإجراءات وإدارة مناسبة.

ج. العناصر الأساسية لأمن نظام المعلومات:

من أجل حماية أمن المعلومات من المخاطر التي تتعرض لها، لابد من توفير مجموعة من العناصر التي يجب أخذها بعين الاعتبار للتوصل إلى تحقيق الحماية اللازمة للمعلومات ويمكن تمثيل هذه العناصر في الشكل الآتي:

الشكل 11: المكونات الأساسية لأمن نظم المعلومات.

المصدر: من إعداد المؤلف.

يمثل الشكل أعلاه العناصر أو المعايير التي هي مجموعة المكونات الواجب توفرها للحفاظ على المعلومات من أي نوع من أنواع الاستغلال والاعتداء، بحيث لا يطلع عليها سوى الأشخاص المصرح لهم حيث أن كل عنصر من هذه العناصر مهم للإبقاء على سرية وسلامة البيانات وإن أي نقص في عنصر

من هذه العناصر سيؤدي حتما إلى المساس بسرية وسلامة المعلومات. وعموما يمكن توضيحها في العناصر التالية:

- ✓ **السرية:** تعرف السرية على أنها حماية البيانات من الانتشار بطريقة غير مرخصة وذلك من خلال منع الأشخاص غير المرخص لهم بالدخول والوصول إلى مصادر المعلومات، وذلك باستخدام عدة معرقلات على سبيل المثال: اسم المستخدم وكلمة السر، بصمة الإبهام، الصوت، العين،....إلخ وهي مهمة في تعريف هوية الشخص ومدى تطابقه مع قاعدة البيانات الخاصة بالمستعملين ومن أجل ضمان سرية المعلومات وحمايتها لابد من تحقيق ما يلي:
  - **تحديد ومراقبة الوصول إلى المعلومات لكي يتمكن فقط الأشخاص المرخص لهم من الاطلاع أو التغيير أو إحداث تعديلات على البيانات.**
  - **القيام بتشفير البيانات من أجل زيادة أمنها وحمايتها أثناء عملية التخزين أو أثناء عملية الإرسال عبر الشبكات مع تزويد الأشخاص المرخصين بمفتاح فك التشفير.**
- ✓ **السلامة:** يقصد بهذا العنصر التأكد من أن تكون المعلومات سليمة في محتواها ولم تتعرض لأي محاولة للإتلاف أو التغيير سواء كانت هذه المحاولة مقصودة أو غير مقصودة، ويجب اتخاذ التدابير اللازمة لحماية المعلومة من التغيير ومن الأمثلة على تغيير محتوى المعلومات تغيير مبلغ التحويل إلى بنك ما من 1000 إلى 100000 مثلا.
- ✓ **الوفرة:** ونقصد بها استمرارية النظام في تقديم الخدمات وتوفير المعلومات الضرورية في الوقت المناسب وبالكمية المناسبة وللشخص المناسب الذي لديه الحق في الوصول إليها، لأن عدم توفر المعلومات عند الحاجة إليها من شأنه أن يؤدي إلى فقدان العديد من المزايا والفرص المتوفرة، ويشكل خطر كبير بالنسبة لمستخدمي هذا النظام ولهذا لابد من اللجوء إلى الأدوات التي تسمح بالتخزين الدوري للبيانات والحفاظ على إتاحة المعلومات واسترجاعها بشكل مستمر.

- ✓ **الحيازة (ضبط الدخول):** ونعني به تحديد السياسات والصلاحيات وتحديد مناطق الاستخدام المسموحة لكل مستعمل وأوقاته لمنع دخول من لا يملك حق شرعي إلى نظام المعلومات سواء من الداخل أو من الخارج.
- ✓ **الأصالة:** يقصد بها التحقق من شخصية وهوية الأشخاص أو الجهات التي تطلع على المعلومات، وهل هم مخولون فعلا ولديهم صلاحيات الوصول والاطلاع على هذا النوع من المعلومات.
- ✓ **عدم الإنكار:** ويعني القدرة على ضمان عدم إنكار الطرف المتعامل معه لوقوع المعاملة والنتائج المترتبة عنها فهي تتعلق بمسؤولية الشخص اتجاه الفعل الذي قد يكون إرسال رسالة أو أي فعل آخر أي لابد من توفر طريقة أو وسيلة لإثبات أي تصرف يوم به أي شخص ومثال ذلك التأكد من وصول بضاعة تم شراؤها عبر شبكة الانترنت إلى صاحبها ولإثبات تحويل المبلغ إلكترونيا يتم استخدام عدة رسائل مثل التوقيع الإلكتروني.

وسائل حماية أنظمة المعلومات

أ. تهديدات أمن نظام المعلومات:

تواجه نظم المعلومات في المنظمات التهديدات الأمنية الآتية:

1. **التهديد الأول:**

الكوارث الطبيعية والسياسية مثل الحرائق، الفيضانات والزلازل، والبراكين، والحروب، وهجمات الإرهابيين. فالكوارث التي لا يمكن التنبؤ بها تستطيع تدمير نظام المعلومات المحاسبي بشكل كامل وتتسبب في فشل المنظمة، ويمكن أن يؤثر حدوث هذه الكوارث في العديد من المنظمات في آن واحد.

2. **التهديد الثاني:**

أخطاء البرمجيات وفشل وظائف المعدات (Equipment functions) مثل فشل المكونات الصلبة للحاسوب (Hardware Failures)، وعطل البرمجيات (Software bugs)، وانهيار نظام التشغيل، وانقطاع وتقلب التيار الكهربائي، وأخطاء إرسال البيانات التي لم يتم الكشف عنها.

3. **التهديد الثالث:**

التصرفات غير المقصودة مثل الحذف والأخطاء غير المقصودة والتي تعرض نظم المعلومات لمخاطر جسيمة وخسائر فادحة. فقد قدرت جمعية أمن نظم المعلومات المحاسبية أن 65% من المشاكل ذات العلاقة بأمن هذه النظم سببها أخطاء العنصر البشري، وأن التصرفات غير العمدية للعنصر البشري تنتج عن الإهمال، والإخفاق في إتباع الإجراءات المرسومة، وضعف تدريب الأفراد والإشراف عليه.

4. **التهديد الرابع:**

التصرفات العمدية أو المقصودة والتي يشار إليها عادة كجرائم للحاسوب، وأغلب أنواع جرائم الحاسوب هو ما يعرف بالخداع أو الحيلة (Fraud) وفيه تكون النية موجهة نحو سرقة شيء ذو قيمة، ومن الأمثلة على جرائم الحاسوب: الكشف غير المصرح به عن البيانات، والعرض غير الصحيح للمعلومات، وتخصيص الموجودات لأغراض غير مصرح بها. ويمكن أن يتخذ هذا النوع من التهديد أيضا شكل التخريب (Sabotage) وتكون النية فيه تحطيم أو إلحاق الأذى بالنظام أو بعض مكوناته.

كما تعددت أشكال الاعتداءات وتنوعت واتخذت طرق وتسميات عديدة منها:

- ✓ **الاعتداء باستعمال البرمجيات الخبيثة:** هي برامج خبيثة تعمل بعيدا دون مساعدة مستعمل الحاسب وهي إما برمجيات متكاثرة (كالفيروسات والديدان)،أو غير متكاثرة كحصان طروادة منها:

- **الفيروسات:** برنامج خبيث يتضمن أهدافا تدميرية لمحتويات الحواسيب المصابة، يتميز بقدرته على نسخ نفسه في البرامج
- **الدودة :** برنامج خبيث قادر على التكاثر والتضاعف والانتقال من حاسوب إلى آخر، هدفها التكاثر والاستنساخ وليس تدمير الحاسوب، وهي تؤدي لاكتظاظ الحاسب المصاب وبطئ سرعة الشبكة.
- **برنامج Macro**: مصمم للعمل على تطبيق واحد مثل Excel،word.
- **القنابل المنطقية**: برنامج يصيب النظام وينتظر حدث ما (كالتاريخ، الأفعال، بيانات خاصة،....الخ).
- **حصان طروادة:** هو برنامج معلوماتي مخبأ في برنامج آخر يقوم بعمليات خبيثة دون علم المستخدم، والقيام بالتحكم في الجهاز، هو يعمل على سرقة كلمة المرور والمعلومات الحساسة.

✓ **الاعتداء باستعمال برامج الجوسسة**: هي برامج خفية عن مستعمل الجهاز تعمل على تسريب المعلومات وإرسالها للخارج بواسطة شبكة الانترنت، كما يمكنها استخدام برنامج **key logger** لتسجيل النقرات على لوحة المفاتيح.

✓ **الاعتداء بأسلوب اعتراض البيانات:** هذه التقنية تعتمد على استراق السمع للبيانات التي تنتقل في شبكة المؤسسة، نذكر منها Sniffer Ettercap.

✓ **الاعتداء باستعمال أسلوب منع الخدمة:** أي الإضرار المادي بالخادم لمنع تقديم الخدمة.

✓ **الاعتداء باستعمال البريد غير المرغوب فيه**: وهذا للإضرار بنظام الرسائل الالكترونية وإرسالها بعشوائية.

✓ **الاعتداء باستعمال أسلوب انتحال العنوان**"IP": أي تعويض عنوانIP الخاص بالمرسل بعنوان آخر وبالتالي اقتحام شبكة المؤسسة.

ب. طرق حماية نظام المعلومات:

تتعدد أوجه الحفاظ على أمن نظم المعلومات وتختلف أشكالها ومنفذيها، ولابد من فهم أن إستراتيجية حماية نظم المعلومات تشكل منظومة متكاملة وبالطبع لا غنى فيها عن استخدام الطرق البرمجية أيضا ويأتي على رأسها: استخدام تقنيات التشفير، جدران الحماية، برمجيات مكافحة الفيروسات، النسخ الاحتياطي ونظم منع وكشف الاختراقات. وهذا ما سيتم تناوله فيما يلي:

1. **التشفير(Encryption):** يعرف التشفير بأنه عملية تشكيل البيانات باستخدام خوارزمية معينة تسمى المفتاح تصبح بها غير قابلة للقراءة إلا بعد استخدام الخوارزمية لفكها. ويتم عادة تشفير البيانات قبل إرسالها عبر الشبكة وذلك لضمان سلامة وصولها دون التعرض لأي عمليات تجسس أو تحريف لمضمونها، على أن يتم فك الشفرة لدى مستقبل الرسالة باستخدام مفتاح فك الشفرة وينبغي الحرص على تشفير البيانات عند الرغبة في إرسالها عبر الشبكة، سواء كانت تلك البيانات كلمات مرور أم أرقام بطاقات الائتمان أم رسائل بريد إلكتروني أم ملف أم غير ذلك. وكلما كانت سرقة البيانات تمثل خطورة كلما كانت هناك ضرورة اكبر لتشفيرها.
2. **الجدران النارية (Firewall):** هي عبارة عن مجموعة من البرمجيات والأجهزة التي يتم إعدادها لتشكيل حدود فاصلة بين شبكة المؤسسة الخاصة انترانت وشبكة الانترنت والهدف منه هو التغلب على اكبر قدر ممكن من الثغرات الأمنية من خلال بناء قناة اتصالات توجه إليها المعلومات المرسلة والمتبادلة مع شبكة الانترنت لمراقبتها والسيطرة على خروجها ودخولها من وإلى شبكة المؤسسة الخاصة وذلك وفق أسس وقواعد يتم تحديدها وبناؤها في جدار النار ، وبالتالي يقوم جدار النار بدور المرشح حيث يراقب تدفقات البيانات التي تمر عبره دخولا وخروجا ويقوم بتحليلها ومن ثم السماح بمرورها إذا كانت تحقق الشروط أو منعها في حالة العكس، ويمكن تقسيم الجدران المقاومة للنار إلى نوعين أساسيين هما:
   - ✓ الجدران البرمجية المقاومة للنار: يمكن استعمال هذا النوع من الجدران على الحسابات المستقلة أو الحاسبات المرتبطة بالشبكة أو على الخوادم؛
   - ✓ الجدران المادية المقاومة للنار: تسمى كذلك بالعلب السوداء وهي تستعمل عادة على الخوادم وهي أكثر أمانا من الجدران البرمجية لكونها غير معنية بنقاط ضعف نظام تشغيل الحاسب ومختلف ثغراته.
3. **برمجيات مكافحة الفيروسات (Virus protection Software)**: البرنامج المضاد للفيروسات هو برنامج يستخدم لمنع واكتشاف فيروسات الحاسوب ، لكن مهما كانت برامج مكافحة الفيروسات مفيدة، فأنه في بعض الأحيان يمكن أن تكون لها عيوب، فيمكن لبرامج مكافحة الفيروسات أن تقلل أداء الحاسوب إذا لم تكن مصممة بكفاءة وقد يواجه المستخدمين غير الخبراء مشكلة في فهم الأوامر والقرارات التي يقدمها برنامج الحماية من الفيروسات وقد يؤدي القرار غير الصحيح إلى الإخلال بالأمن. وتتواجد في أسواق البرمجيات العديد من البرمجيات المضادة للفيروسات، ويجب معرفة أن هذه البرمجيات تفقد قيمتها في ظل عدم وجود تحديثات

مستمرة **Updating** ، للحصول على قاعدة بيانات جديدة حول الفيروسات التي لا تتوقف عن التمحور والظهور بأسماء وأشكال تهديد مختلفة على مدار الوقت

4. **النسخ الاحتياطي (Backup):** على الرغم من الاحتياطات الأمنية المتعددة التي قد تتبع لحماية البيانات إلا انه من المحتمل وقوع أي نوع من التلف أو التحريف أو الفقدان للبيانات، لذا كان لابد من تأمين طريقة يمكن من خلالها استعادة البيانات التالفة أو المفقودة أو المحرفة لضمان مستوى أعلى من الحماية للنظام .ويحقق النسخ الاحتياطي للبيانات هذا المستوى من الحماية، حيث يتم من خلاله إنشاء نسخ احتياطية يتم حفظها سواء في نفس مقر العمل أو خارجه، ويتم تحديثها بصورة منتظمة لضمان أقل قدر من الخسائر في حالة فقدان البيانات الأصلية.
5. **أدوات منع وكشف الاختراقات(Intrusion Prevention/Detection Systems):** تضاف أدوات صد أو منع الاختراقات إلى مستويات الحماية التي يجب توفيرها للنظم، وتعتبر هذه الإضافات بمثابة حماية مبكرة للنظام ولكن فيما لو تمكن مهاجم أو برنامج محدد من إحداث خلل بالنظام فإن أدوات أخرى يجب استخدامها تسمى أدوات الكشف عن الاختراقات، ويجب أن يتم فحص هذه الوسائل من فترة لفترة حتى يتمكن النظام من العمل بفعالية، كما أنها تفيد مسؤولي النظم في توظيف التقارير التي تنتجها النظم آليا في وضع إحصائيات محددة ووضع تصورات حول أنشطة النظام وأمنه، وتختلف عن الجدران النارية بأنها تحتاج إدارة ومتابعة أكبر من قبل مراقبي نظم المعلومات والقائمين على تتبع أمن نظم المعلومات.